

# **Information Operations Across Infospheres**

**Annual Report**

**Prepared by**

**The University of Texas at Dallas**

**Submitted to:  
Air Force Office of Scientific Research**

**November 20, 2007**

**Under  
Contract: FA9550-06-1-0045**

**Period of Performance:  
December 1, 2006 – November 2007, 2007**

**Subcontractor:  
George Mason University  
(Currently at  
The University of Texas  
At San Antonio)**

## EXECUTIVE SUMMARY OF PROJECT

There is a critical need for organizations to share data within and across infospheres and form coalitions so that analysts could examine the data, mine the data, and make effective decisions. Each organization could share information within its infosphere. An infosphere may consist of the data, applications and services that are needed for its operation. Organizations may share data with one another across what is called a global infosphere that spans multiple infospheres. It is critical that the war fighters get timely information. Furthermore, secure data and information sharing is an important requirement. The challenge is for data processing techniques to meet timing constraints and at the same time ensure that security is maintained.

This proposal addresses information operations across infospheres. We first describe secure timely data sharing across infospheres and then focus on Role-based access control and Usage control in such an environment. Our goal is to send timely information to the war fighter while maintaining security. We will also address the application of game theory as well as decision centric data mining techniques to extract information from both trustworthy and untrustworthy partners of the coalition.

In particular, the **objectives** of this project are as follows:

- Develop a Framework for Secure and Timely Data Sharing across Infospheres.
- Investigate Access Control and Usage Control policies for Secure Data Sharing.
- Develop innovative techniques for extracting information from trustworthy and untrustworthy partners.

**Technical Merit:** While there has been work on data sharing across coalitions, an in-depth investigation of security issues as well as a study of the tradeoffs between security and timely processing has yet to be carried out. To our knowledge, this project is the first to investigate sophisticated security techniques such as Usage Control as well as decision centric data mining techniques for timely and secure data sharing across coalitions.

**Broader Impact:** The research to be carried out on this project is directly applicable to Network Centric Operations (NCO) that implement Network Centric Warfare (NCW). NCW promotes information sharing, shared situational awareness and knowledge of commander's intent. In addition it also enables war fighting advantage by providing synchronization, speed of command and increased combat power. We focus mainly on information sharing aspects of NCW. In particular, the results of this project can be transferred to the timely and secure data sharing services of the Network Centric Services activity being carried out by the Department of Defense.

**Research Team:** The research will be carried out both at the University of Texas at Dallas and at George Mason University. The principal investigators are among the leading researchers in Data and Applications Security. They have conducted innovative research in Secure Database Design, the Inference Problem, Role-based Access Control and Usage Control techniques as well as and carried out technology transfer activities. They are Fellows of IEEE, ACM, AAAS and the British Computer Society and have received prestigious awards for their research in Data and Applications Security.

# ABSTRACT OF ANNUAL REPORT

The research reported in this annual report was carried out at mainly the University of Texas at Dallas (UTD) between December 1, 2006 and November 20, 2007. It describes the issues and challenges for information operations across infospheres and focuses on assured information sharing. We have examined three models: In the first model the partners of the coalition are considered to be trustworthy. In the second model, the partners are semi-trustworthy. In the third model the partners are untrustworthy.

The report essentially consists of three four parts; three of which are produced by members of the UTD team and one is produced by members at GMU (now UTSA) team. We first provide an introduction to the project as well as the developments during Year 2. This introduction was also presented at the AFOSR review in June 2007. In the case of trustworthy models we conducted experiments on data sharing vs. data policy enforcement and developed a prototype systems based on the concepts developed during Year 1. This work is published as a UTD Technical Report (Part 1). For the semi-trustworthy model we examined the use of game theory for extracting information from the partners. We enhanced the research carried out during Year 2. This research is published in a UTD Technical Report (Part II). For the untrustworthy model, we examined the use of data mining for defensive operations. This research is published in a UTD Technical Report (Part III).

In addition to the above, George Mason University (GMU) received a subcontract from the University of Texas at Dallas to examine the use of Role-based Access Control (RBAC) and Usage Control models for Coalition data sharing. The research was carried out at GMU between January and May 2007. This research is in the form of a presentation and is included in the report (Part IV). This subcontract has now moved to the University of Texas at San Antonio (UTSA) since the PI has moved to UTSA from GMU.

## **ACKNOWLEDGEMENT**

Much of the research discussed in this annual report was supported buy the Air Force office of Scientific Office under Contract FA9550-06-1-0045. We thank Dr. Robert Herklotz of AFOSR for funding his encouragement and motivation. This research as also partially supported by the Erik Jonsson School of Engineering and Computer Science at the University of Texas at Dallas under the Texas Enterprise Funds. We thank Prof. Robert Helms (Dean) and Prof. Andrew Blanchard (Senior Associate Dean) for this support.

# Table of Contents

**Introduction:**  
**Information Operation across Infospheres**

**Part I:**  
**Architecture for a Trusted Computing base**  
*For need-to-share in case of emergencies*

**Part II:**  
**Enforcing Honesty in Assured Information Sharing within a Distributed System**

**Part III:**  
**Data Mining for Defensive Operations**

**Part IV:**  
**The Secure Information Sharing Problem and Solution Approaches**